

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Tsuyoshi YOSHIZAWA et al.

Serial No.: 10/620,313

Filed: July 15, 2003



Group Art Unit:

Examiner:

For: MAGNETIC DISK MEDIUM, FIXED MAGNETIC DISK DRIVE UNIT AND
METHOD THEREOF

Certificate of Mailing

I hereby certify that this paper is being deposited with the
United States Postal Service as first class mail in an
envelope addressed to: Commissioner for Patents, P.O.
Box 1450, Alexandria VA 22313-1450 on:

Date: 08/05/03

By: [Signature]

Marc A. Rossi

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the
following country is hereby requested for the above-identified application and the priority
provided in 35 U.S.C. § 119 is hereby claimed:

JAPAN 2002-205886 - July 15, 2002

In support of this claim, a certified copy of said original foreign application is filed
herewith. It is requested that the file of this application be marked to indicate that the
requirements of 35 U.S.C. 119 have been fulfilled and that the Patent and Trademark Office
kindly acknowledge receipt of this document.

Respectfully submitted,

08/05/03
Date

[Signature]
Marc A. Rossi
Registration No. 31,923

Attorney Docket: FUJI:262

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2002年 7月15日

出願番号
Application Number:

特願2002-205886

[ST.10/C]:

[JP2002-205886]

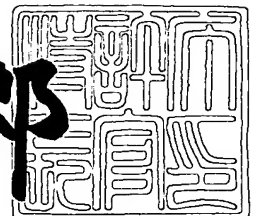
出願人
Applicant(s):

富士電機株式会社

2003年 2月21日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3009743

【書類名】 特許願

【整理番号】 02P01092

【提出日】 平成14年 7月15日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 5/82
G11B 19/04

【発明者】

【住所又は居所】 神奈川県川崎市川崎区田辺新田 1 番 1 号 富士電機株式会社内

【氏名】 由沢 剛

【発明者】

【住所又は居所】 神奈川県川崎市川崎区田辺新田 1 番 1 号 富士電機株式会社内

【氏名】 佐藤 公紀

【特許出願人】

【識別番号】 000005234

【氏名又は名称】 富士電機株式会社

【代理人】

【識別番号】 100088339

【弁理士】

【氏名又は名称】 篠部 正治

【手数料の表示】

【予納台帳番号】 013099

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9715182

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 磁気ディスク媒体及び固定磁気ディスク装置

【特許請求の範囲】

【請求項 1】 記録領域に凹凸部からなるプリフォーマット領域と凹部又は凸部からなる非プリフォーマット領域が設けられているプリエンボス型磁気ディスク媒体であって、該磁気ディスク媒体を一意に識別するための ID 情報が前記記録領域内に記録されており、さらに該 ID 情報が前記プリフォーマット領域内の第 1 の ID 情報と、前記非プリフォーマット領域内の第 2 の ID 情報により構成されていることを特徴とする磁気ディスク媒体。

【請求項 2】 請求項 1 に記載の磁気ディスク媒体において、前記プリフォーマット領域において前記第 1 の ID 情報を形成する凹凸部は、凹部の深さが前記磁気ディスク媒体を内蔵する固定磁気ディスク装置の記録ヘッドのギャップから発生する磁界により磁化方向を反転不能な十分な深さに設定されていることを特徴とする磁気ディスク媒体。

【請求項 3】 請求項 1 に記載の磁気ディスク媒体において、前記第 1、第 2 の ID 情報は、前記磁気ディスク媒体の記録面毎に記録され、さらに各情報がそれぞれ異なる ID 情報を有することを特徴とする磁気ディスク媒体。

【請求項 4】 請求項 1 に記載の磁気ディスク媒体において、前記第 1 及び第 2 の ID 情報は、所定の暗号方式により暗号化された情報であることを特徴とする磁気ディスク媒体。

【請求項 5】 請求項 1 に記載の磁気ディスク媒体において、前記第 1、第 2 の ID 情報は、識別情報としての ID 情報本体と、そのデジタル署名情報を含むことを特徴とする磁気ディスク媒体。

【請求項 6】 請求項 1 に記載の磁気ディスク媒体を 1 枚以上内蔵した固定磁気ディスク装置であって、前記磁気ディスク媒体の前記第 1、第 2 の ID 情報を読み出すための読出し手段と、前記第 1、第 2 の ID 情報の暗号を解除する暗号解除手段と、前記第 1、第 2 の ID 情報をデジタル署名情報に基づきチェックするチェック手段と、前記第 1、第 2 の ID 情報のペアを上位装置に転送する転送手段とを備えることを特徴とする固定磁気ディスク装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、磁気ヘッドによりデジタル情報を記録再生する固定磁気ディスク装置と磁気ディスク媒体に関するものであり、特に磁気ディスク媒体にメディアの識別情報を埋め込むことによりセキュリティ機能を加えた固定磁気ディスク装置とその磁気ディスク媒体に関する。

【0002】

【従来の技術】

固定磁気ディスク装置は高速で回転する磁気ディスク基板上を磁気ヘッドがサブミクロンオーダーの間隔を保って浮上しながら、信号の記録再生を行っている。固定磁気ディスク装置に用いられる従来の磁気ディスク基板は、アルミやガラス等の非磁性体を材料とする平坦な基板上に、磁性層と保護膜を積層して作られていた。ところが近年、基板上に設けられた凹凸パターンにサーボ情報等のプリフォーマット情報を記録するプリエンボス方式の磁気ディスクが一部の固定磁気ディスク装置に用いられるようになっている。

【0003】

例えば日経エレクトロニクスNo. 586(1993. 7. 19)に紹介されている固定磁気ディスク装置は、サーボパターンと記録トラックを凹凸形状でガラス基板上に形成したプリエンボス媒体を用いている。本媒体のサーボパターンは凹部と凸部がトラック方向に沿って互いに逆向きに磁化されており、凹凸の境界部分から漏れ出る磁束を磁気ヘッドで検出し、1/0の信号パターンを読み取っている。

【0004】

このようなプリエンボス方式磁気ディスクは光ディスクと同様の製造方法を用いるので、サーボ情報や記録トラックを精度良く形成できるのが特徴である。

なお、本方式はサーボパターンへの用途以外に、例えばプログラムやデータ等をあらかじめ格納したROMディスクへの用途が期待されている。

ところで昨今、画像データ、音声データ、様々なソフトウェアデータ（以下、

これらをコンテンツと呼ぶ)が、インターネット等のネットワークを介して流通している。これらのコンテンツをネットから購入、ダウンロードした際にそのデータを一時的に保存するための手段として固定磁気ディスク装置やメモ리카ードが用いられている。

【 0 0 0 5 】

また、デジタルコンテンツの流通量の増大に伴い、コンテンツを保護するための仕組みとしてデジタル著作権管理システムが導入されている。デジタル著作権管理システムは、顧客が購入したコンテンツに何らかの操作を施すことで、このコピーを第三者に渡したり、インターネットにアップロードして配布したりすることができないようにするものである。

【 0 0 0 6 】

ある種のデジタル著作権管理システムは、コンテンツを再生するクライアント PC のハードウェア情報をベースにキーを生成して、そのキーが無いと再生できないような仕組みを提供している。例えばスマートカード (インテリジェント機能を備えるメモ리카ード) と連携した或るシステムは、ハードウェア情報としてスマートカード内に埋め込まれたカード固有の ID 情報を用いる。この ID 情報は改竄できないような状態で埋め込まれており、これにより高いセキュリティ性を実現している。

【 0 0 0 7 】

【発明が解決しようとする課題】

一方、固定磁気ディスク装置において、上述したような ID 情報をメディアに埋め込んだ例はこれまで見られなかった。固定磁気ディスク装置は構造上内部データの書き換えが比較的容易なことなことがその一つの理由となっている。すなわち ID 情報を磁気ヘッドでソフト的に埋め込む方法では、不正使用を目的とする ID 情報の改竄を防ぐことが難しい。

【 0 0 0 8 】

その解決策として上述したプリエンボス型磁気ディスクにより、ID 情報をハード的に埋め込む方法が考えられる。しかしスタンパで成型するプリエンボス型磁気ディスクでは、同一スタンパで成型した磁気ディスクが同一の ID 情報を有

するという問題がある。すなわち I D 情報の一意性を保つことができない。

本発明は、上述の点に鑑み、改竄が困難であると共に、一意性の有る I D 情報を埋め込むことが可能な磁気ディスク媒体と、これを適用することでセキュリティ機能を付加した固定磁気ディスク装置とを提供することを目的とする。

【 0 0 0 9 】

【課題を解決するための手段】

上述の目的を達成するため、本発明の磁気ディスク媒体は、記録領域に凹凸部からなるプリフォーマット領域と凹部又は凸部からなる非プリフォーマット領域が設けられているプリエンボス型磁気ディスク媒体であって、該磁気ディスク媒体を一意に識別するための I D 情報が前記記録領域内に記録されており、さらに該 I D 情報がプリフォーマット領域内の第 1 の I D 情報と、非プリフォーマット領域内の第 2 の I D 情報により構成されていることを特徴としている。

【 0 0 1 0 】

ここで、プリフォーマット領域内の第 1 の I D 情報と非プリフォーマット領域内の第 2 の I D 情報から構成される I D 情報は、改竄が困難であると共に一意性を有する情報となる。

また、上記磁気ディスク媒体において、プリフォーマット領域内の前記第 1 の I D 情報を形成する凹凸部は、凹部の深さが前記磁気ディスク媒体を内蔵する固定磁気ディスク装置の記録ヘッドのギャップから発生する磁界により磁化方向を反転不能な十分な深さに設定されていることが好ましい。これで固定磁気ディスク装置のヘッドにより、少なくとも凹部を書き換えることができなくなる。すなわち不正使用者がマスタ I D 情報を自分の意図する内容に変更することが困難になる。

【 0 0 1 1 】

また、上記磁気ディスク媒体において、前記第 1、第 2 の I D 情報は、前記磁気ディスク媒体の記録面毎に記録され、さらに各情報がそれぞれ異なる I D 情報を有することが好ましい。複数の I D 情報が利用可能となるため、より柔軟なセキュリティ管理が可能となり、本磁気ディスク媒体の有用性を高めることができる。

【0012】

また、上記磁気ディスク媒体において、前記第1及び第2のID情報は、所定の暗号方式により暗号化された情報であることが好ましい。暗号化により固定磁気ディスク装置の分解調査によるID情報の漏洩が防止される。

また、上記磁気ディスク媒体において、前記第1、第2のID情報は、識別情報としてのID情報本体と、そのデジタル署名情報を含むことが好ましい。デジタル署名情報によりID情報の不正な改竄が検知されるため、ID情報の信頼性を高めることができる。

【0013】

また、本発明の固定磁気ディスク装置は、上述の目的を達成するため、本発明の磁気ディスク媒体を1枚以上内蔵した固定磁気ディスク装置において、前記磁気ディスク媒体の前記第1、第2のID情報を読み出すための読出し手段と、前記第1、第2のID情報の暗号を解除する暗号解除手段と、前記第1、第2のID情報をデジタル署名情報に基づきチェックするチェック手段と、前記第1、第2のID情報のペアを上位装置に転送する転送手段とを備えることを特徴とする。

【0014】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態を詳細に説明する。

図5に本発明の実施形態の固定磁気ディスク装置の構成を示す。固定磁気ディスク装置5は、筐体11の上に磁気ヘッド14を支持するアーム15、アーム15を固定する櫛歯状のキャリッジ16、及びこれを駆動するボイスコイルモータ17、及び磁気ディスク1が取り付けられている。磁気ディスク1は複数積層されてスピンドル軸12に固定されている。スピンドル軸12は筐体11の下側に取り付けられている図示しないスピンドルモータにより一定の角速度で回転する。キャリッジ16はボイスコイルモータ17によりシャフト13を中心に揺動運動する。磁気ヘッド14は各ディスク面に対向するようにアーム15の先端に取り付けられ、キャリッジ16の移動に伴って回転するディスク上を浮上しながら移動するようになっている。

【 0 0 1 5 】

図 2 は本発明の磁気ディスク媒体の実施形態である磁気ディスクの平面図である。磁気ディスク 1 は記録情報の一部が凹凸部で形成されたプリエンボス型磁気ディスクであり、基板材料として合成樹脂等が使用され、その上に磁性膜と保護膜が積層されている。本磁気ディスク 1 の記録面には制御情報が記録されたサーボゾーン 2 が放射状に設けられており、またデータを記録するための同心円状のトラックが設けられている。

【 0 0 1 6 】

図 6 は磁気ディスク 1 の記録面の詳細図である。図においてドット模様を施した領域は凸部、白抜き部分は凹部、それ以外は凹凸部となっている。

サーボゾーン 2 には、トラック位置を特定するためのトラック ID 2 6、及びヘッドの位置のトラック中心からの位置ずれを検知するための格子パターン 2 3、及びその他の制御情報が凹凸で形成されている。

【 0 0 1 7 】

サーボゾーン 2 により分割されるような形でトラックが敷設されている。また隣接トラックからの干渉を防止するためのガードバンド 2 8 が凹部によりトラック間に形成されている。トラックには凸部のみで形成されたものと、凹凸部で形成されたものがある。凸部のみで形成されたトラック、例えばトラック 2 7 等はプリフォーマットされていない（すなわちデータの読み書きが可能な）トラックであり、凹凸部で形成されたトラック 2 9 はプリフォーマットされた（再生専用の）トラックである。

【 0 0 1 8 】

プリフォーマット及び非プリフォーマットトラックは共に論理的なフォーマットが施されている。すなわち読み書きの基本単位であるセクタに分割されている。各々のセクタはデータ本体とヘッダ情報、及び誤り訂正用の冗長バイトがから構成されている。ヘッダ情報にはそのセクタのアドレス情報や、データに同期したクロックを生成するための同期情報等が含まれている。またデータ本体は連続する 0 の数を制限した符号形式（例えば 2-7 RLL 符号等）に変換されている。

【 0 0 1 9 】

上述した磁気ディスク 1 は光ディスクの製造方法を用いて製造することができる。図 4 はその手順を示したものである。まずガラス円盤 9 0 を研磨してキズの無い、平坦な状態に仕上げる。そしてその上に感光剤（レジスト） 9 1 を塗布する。そしてレーザーカッティング装置にてレーザー光を記録するパターンに応じて断続しながら照射する。これを現像するとレーザー光が照射された部分は溶けて、表面にパターンに応じたくぼみができる。さらにその表面にニッケルを厚くメッキしスタンパ 9 4 を型取りする。さらにスタンパ 9 4 を型にして合成樹脂材料を射出成型し、基板 9 5 を成型する。最後に基板 9 5 の表面にスパッタ等により磁性層と保護膜を積層すると磁気ディスクが完成する。

【 0 0 2 0 】

さらに本磁気ディスクは着磁という操作を行うことにより磁気ヘッドにて信号パターンの検出が可能となる。着磁は図 1（a）に示すようにまず、強い磁界を発生する磁気ヘッドにより凹凸の上部、下部共にある一方向に着磁を行い（一次着磁）、その後図 1（b）のように一次着磁より弱い適正な磁界を発生する磁気ヘッドにより逆方向に着磁する（二次着磁）。二次着磁では凹部は反転されないため、凹凸部の境界で磁化遷移が発生するようになる。

【 0 0 2 1 】

磁気ヘッドが浮上しながらこの凹凸部を通過する際、磁化遷移の部分で磁化遷移方向に応じて正又は負ピークを持つ電圧信号が発生するため、この電圧信号を増幅してピーク検知すれば信号パターンが読み取れる。

図 3 に示したように本磁気ディスクの記録面には、所定のトラック位置に 2 種類の I D 情報（マスタ I D 情報 3 及びメディア個別 I D 情報 4）が記録されており、これによりメディアを一意に識別できるようになっている。

【 0 0 2 2 】

マスタ I D 情報 3 はあらかじめスタンパに埋め込まれており、成型工程でスタンパから磁気ディスクに凹凸パターンとして転写されるものである。従って同一のスタンパにより成型された磁気ディスクは同一のマスタ I D 情報を有する。マスタ I D 情報 3 はスタンパを一意に識別するためのマスタ I D を含む。マスタ I

Dは例えばスタンプのシリアル番号等を用いることができる。異なるマスタID情報を埋め込んだ2枚のスタンプを用いて、磁気ディスクの表裏の記録面の成型を行うことにより、記録面毎に異なるマスタID情報を作成することもできる。

【0023】

マスタID情報3をスタンプに凹凸パターンとして埋め込む場合には暗号化を施すことが好ましい。これにより固定磁気ディスク装置の分解調査による解析がさらに困難となる。使用する暗号方式としてはこの場合特に制約は無い。

また、マスタID情報3にはマスタIDのデジタル署名情報が含まれていることが望ましい。このデジタル署名はマスタIDが正規の製造者により作成されているか否か、及びそのマスタIDが改竄されているか否かを検証できるようにするものである。

【0024】

このデジタル署名は、マスタIDをハッシュ関数により固定長データ（ハッシュコード）に変換した後、公開鍵暗号方式における秘密鍵を使用してハッシュコードを暗号化することにより作成することができる。これをチェックする場合は、まず磁気ディスクからマスタIDとデジタル署名を読み込み、デジタル署名を上記の秘密鍵の対をなす公開鍵により暗号化解除してハッシュコードを得る。そしてこのハッシュコードをマスタIDからハッシュ関数により求めたハッシュコードと比較し、一致／不一致を判定する。判定の結果一致していればマスタIDが正規の製造者により作成され、かつその改竄は行われていないと推定される。

【0025】

このマスタID情報3は、図6に示す凹凸部からなるプリフォーマットされたトラック（再生専用トラック29）に埋め込まれる。この再生専用トラック29は磁気ディスク1内の任意のトラック位置に設けることができる。

再生専用トラック29の凹凸形状において、凹部の深さは固定磁気ディスク装置の記録ヘッドのギャップ部から発生する記録磁界が凹部に十分に届かない深さに設定することが好ましい。その最適値は使用するヘッドの特性やヘッド浮上量等により変わる。そのため凹部の深さは固定磁気ディスク装置のハード仕様に合

わせて最適値を選ぶ。

【 0 0 2 6 】

図 7 はマスタ I D を埋め込んだスタンプを製作する過程で用いる製造装置 3 1 の構成を示したものである。本装置はレジストを塗布したガラス基板の表面に凹凸に応じたパターンを書き込むために使用される。次に本製造装置の動作について説明する。

まずマスタ I D 発生器 3 2 は一意な I D 番号、例えば 1 0 5 7 2 9 7 2 を発生し、暗号化器 3 3 は外部から入力される共通鍵 9 6 によりこれを暗号化する。ハッシュ関数演算器 3 4 は所定のハッシュ関数演算により暗号化されたマスタ I D を例えば 1 2 8 バイトの固定長ハッシュコードに変換する。さらに暗号化器 3 5 は外部から入力される秘密鍵 9 7 によりこのハッシュコードを暗号化しデジタル署名 3 6 を作成する。

【 0 0 2 7 】

暗号化されたマスタ I D 3 7 とデジタル署名 3 6 は結合されフォーマット変換器 3 8 に入力される。フォーマット変換器 3 8 はバイト形式の入力データをシリアルビット列に変換すると共に、トラックの論理フォーマットに合わせてフォーマット変換を行い、さらに所定の符号形式への変換を行う。さらにマッピング演算器 3 9 はフォーマット変換器 3 8 の出力データを、マスタ I D 情報を記録するトラック位置に基づいて 2 次元領域にマッピングし、マスタ I D 情報の凹凸パターン情報を生成する。

【 0 0 2 8 】

レーザーカティング装置 4 0 はサーボゾーンや記録トラックの凹凸パターン情報を格納したマスタデータ 4 1 と、マッピング演算器 3 9 の生成した凹凸パターン情報 3 9 a を入力する。そして感光体を表面に塗布したガラス基板 9 0 を回転させながら、これらの入力情報に基づいてレーザー 4 2 の ON / OFF を行う。さらにこのガラス基板 9 0 を現像し、その表面に形成された凹凸にニッケルメッキ処理を施すことによりスタンプが完成する。

【 0 0 2 9 】

マスタ I D 情報は上述したように磁気ヘッドで任意情報に変更することが困難

なため、耐タンパ性に優れるという利点がある。しかしその反面、同一のスタンパから製造された磁気ディスクが同一の I D 情報を有することになるため、一意性が保てないという欠点がある。この欠点を補うため本発明の磁気ディスクは、第 2 の I D 情報としてメディア個別 I D 情報を使用する。メディア個別 I D 情報は、磁気ディスクを一意に識別する I D 番号を含む。

【 0 0 3 0 】

磁気ディスクの表裏の記録面に異なるメディア個別 I D 情報を記録することができる。これにより 1 枚の磁気ディスクで複数の I D 情報が利用可能となるため、より柔軟なセキュリティ管理が可能となる。

また、マスタ I D 情報と同様に本 I D 情報も磁気ディスクに書き込む際に暗号処理を施すことが望ましい。この場合も同様に使用する暗号方式に特に制約は無い。またマスタ I D 情報と同様にメディア個別 I D 情報にもデジタル署名情報が含まれていることが望ましい。

【 0 0 3 1 】

このメディア個別 I D 情報は図 6 の再生専用トラック 2 9 を除くトラック、すなわちプリフォーマットされていないトラック（トラック 2 7 等）に磁気ヘッドで記録される。ここでトラック位置に特に制約は無い。製造工程において本 I D 情報を記録する処理は固定磁気ディスク装置の組み立てが全て完了した後に行われる。

【 0 0 3 2 】

図 9 は固定磁気ディスク装置 5 に内蔵されている磁気ディスク 1 に個別メディア I D 情報を書き込む装置の構成を示したものである。図のように書込みは I D 書込み装置 7 0 と固定磁気ディスク装置 5 をバス 6 2 により接続しておこなう。

図において I D 書込み装置 7 0 はメディア個別 I D 発生器 7 1 が生成するメディア固有の I D 番号 7 1 a を、暗号化器 7 2 で暗号化し、暗号データ 7 9 を作成すると共に、ハッシュ関数演算器 7 3 と暗号化器 7 4 によりそのデジタル署名 7 8 を生成し、これらを合わせたライトデータ 8 2 を作成する。ライトデータ 8 2 と共にトラック番号及びヘッド番号 7 7 を固定磁気ディスク装置 5 に書込みの指令として送ることにより磁気ディスク 1 の所定トラックの所定記録面にメデ

ア個別 I D 情報 4 が書き込まれる。

【 0 0 3 3 】

図 8 は本発明の実施形態の固定磁気ディスク装置の制御部 5 0 の構成図である。本制御部 5 0 のヘッドアンプ 5 1 はヘッド再生信号を増幅するリードアンプ（図省略）、磁気ヘッド 1 4 の記録電流のスイッチングを行うドライバ回路（図省略）、及びヘッド選択回路等（図省略）から構成されている。ヘッドアンプ 5 1 の出力信号は読出し制御部 5 3 に導かれ、ここでデータの再生が行われる。読出し制御部 5 3 は、再生信号のピーク検出を行うピーク検出回路 5 3 a、チャネル符号化されたデータの復号化を行う復調回路 5 3 b 等を含む。フォーマット制御部 5 6 は所定のセクタフォーマットに基づくリード／ライトデータのフォーマット変換、誤り訂正符号によるリードデータのチェック、誤り発生時の訂正処理等を行う。バッファメモリ 6 3 はリード・ライトするデータを一時的に格納するためのメモリである。

【 0 0 3 4 】

本固定磁気ディスク装置はバス 6 2 を介して上位装置 6 1（例えば P C）と接続されている。C P U 5 8 は上位装置 6 1 から送られてくるコマンドを解析し、各コマンドの処理を実行する。

R O M 5 8 a は本装置のファームウェアを記憶したリードオンリーメモリである。R O M 5 8 a にはさらに、I D 情報を読み出す際に必要となる幾つかの鍵データを保管した鍵テーブル 1 0 1 が記憶されている。図 1 1 は鍵テーブル 1 0 1 の内容を示したものである。マスタ I D 用共通鍵 1 0 1 a は、図 7 のスタンパ製造装置において暗号化器 3 3 に入力される共通鍵 9 6 と同一の鍵、マスタ I D 用公開鍵 1 0 1 b は暗号化器 3 5 に入力される秘密鍵 9 7 と対をなす公開鍵となっている。またメディア個別 I D 用共通鍵 1 0 1 c は、図 9 の I D 情報記録装置 7 0 において暗号化器 7 2 に入力される共通鍵 9 8 と同一の鍵、メディア個別 I D 用公開鍵 1 0 1 d は暗号化器 7 4 に入力される秘密鍵 9 9 と対をなす公開鍵である。

【 0 0 3 5 】

図 1 0 は本発明の固定磁気ディスク装置において磁気ディスクに格納された I

D 情報を読み出す場合の手順を示したフローチャートである。ここで固定磁気ディスク装置 5 は電源投入後のイニシャライズ処理が完了し、上位装置 6 1 からのコマンド待ち状態であると仮定している。次に I D 情報の読み出しの手順を本フローチャートと、図 8、図 1 1 等を用いて説明する。

【 0 0 3 6 】

上位装置 6 1 からバス 6 2 を介して特定のヘッド番号の I D 情報の読出し指令が送られてくると、まず S 1 において C P U 5 8 は位置決め制御部 5 4 に指令を送り、ヘッド 1 4 をマスタ I D 情報が格納されているトラック（再生専用トラック）へシークさせる。

S 2 において、C P U 5 8 はヘッドアンプ 5 1 に指令を送り複数のヘッドの中から上位装置 6 1 が指定したヘッドを選択する。するとそのヘッドに対応する記録面からの再生信号がヘッドアンプ 5 1 で増幅され、その出力がピーク検出回路 5 3 a を介して復調回路 5 3 b へ導かれ、復調回路 5 3 b から再生専用トラックのデータが N R Z データ列として読み出される。

【 0 0 3 7 】

S 3 において、C P U 5 8 はフォーマット制御部 5 6 にマスタ I D 情報の読出しを指示する。すると N R Z データ列はフォーマット制御部 5 6 に入力され、ここでマスタ I D 情報が格納されたセクタのデータのみが抽出され、さらにフォーマット制御部 5 6 により本セクタデータの誤りチェック、必要に応じた誤り訂正が行われ、その後セクタデータが転送制御回路 5 7 を介してバッファメモリ 6 3 に保存される。

【 0 0 3 8 】

S 4 において、C P U 5 8 はまずバッファメモリ 6 3 にアクセスし、セクタデータ内のデジタル署名データを鍵テーブル 1 0 1 に格納されてマスタ I D 用公開鍵 1 0 1 b を用いて暗号化解除する。次に所定のハッシュ関数によりセクタデータ内のマスタ I D データのハッシュコードを計算する。ここで所定のハッシュ関数は図 7 のスタンパ製造装置におけるハッシュ関数演算器 3 4 に適用される関数と同一の関数となっている。

【 0 0 3 9 】

S 5において、CPU 5 8は前ステップにおけるデジタル署名を暗号化解除したコードと、マスタIDから計算したハッシュコードを比較する。ここでもしこれらが異なっていた場合は、メディアに何らかの異常があると判断し、上位装置へ異常の発生を通知する（S 1 4）。そして処理を中断してコマンド待ち状態に戻る（S 1 3）。

【0 0 4 0】

そうでない場合は、次のステップS 6に進む。S 6において、CPU 5 8は暗号化されたマスタID用共通鍵1 0 1 aにより暗号化解除する。そして平文化されたマスタID（1 6ビット）を取得する。

次にS 7において、CPU 5 8は磁気ヘッド1 4をメディア個別ID情報が格納されているトラックヘシークさせる。

【0 0 4 1】

さらにS 8において、本トラックに記録されたID情報の読出しが実行され、メディア個別ID情報を含むセクタデータがバッファメモリ6 3に読み込まれる。

S 9において、CPU 5 8はまず、セクタデータ内のデジタル署名データをメディア個別ID用公開鍵1 0 1 dを用いて暗号化解除する。次に所定のハッシュ関数によりセクタデータ内のメディア個別IDのデータのハッシュコードを計算する。ここで所定のハッシュ関数は図9のID情報記録装置におけるハッシュ関数演算器7 3に適用される関数と同一の関数となっている。

【0 0 4 2】

次にS 9において、CPU 5 8は前ステップにおけるデジタル署名を暗号化解除したコードと、メディア個別IDから計算したハッシュコードを比較する。ここでもしこれらが異なっていた場合は、メディアに何らかの異常があると判断し、S 1 4で上位装置へ異常の発生を通知する。そして処理を中断してコマンド待ち状態に戻る。

【0 0 4 3】

そうでない場合は、次のステップS 1 1に進む。S 1 1において、CPU 5 8は暗号化されたメディア個別IDをメディア個別ID用共通鍵1 0 1 cにより暗

号化解除する。そして平文化されたメディア個別ID(32ビット)を取得する。最後にS12において、CPU58はマスタID(16ビット)とメディア個別ID(32ビット)を結合し、48ビットのIDを作成する。そしてこれをバス62を介して上位装置61に送る。そしてその後、S13で上位装置61からのコマンド待ち状態に戻る。

【0044】

上位装置61はその後必要に応じて、その他のヘッドに対しても同様にIDの読出しコマンドを送る。そして各ヘッドに対応するIDを取得し、これらを元に暗号鍵の生成等を行う。

【0045】

【発明の効果】

以上説明したように本発明の磁気ディスク媒体によれば、メディアを一意に識別するためのID情報を、プリエンボス型磁気ディスクのプリフォーマット領域と、非プリフォーマット領域とに分けて記録するようにしたため、改竄が困難であると共に一意性の有るID情報を記録した磁気ディスク媒体を提供可能となる。

【0046】

また、本発明の固定磁気ディスク装置によれば、上記磁気ディスク媒体を1枚以上内蔵し、本磁気ディスク媒体からID情報を読み出して上位装置に転送することができるため、様々なセキュリティシステムに適用可能な固定磁気ディスク装置を提供可能となる。

【図面の簡単な説明】

【図1】

本発明の実施形態の磁気ディスクの初期磁化の原理説明図で、(a)は一次着磁を示し、(b)は二次着磁を示す。

【図2】

本発明の実施形態の磁気ディスクの平面図(その1)である。

【図3】

本発明の実施形態の磁気ディスクの平面図(その2)である。

【図 4】

本発明の実施形態の磁気ディスクの製造方法の説明図である。

【図 5】

本発明の実施形態の固定磁気ディスク装置の構成図である。

【図 6】

本発明の実施形態の磁気ディスクの記録面の詳細図である。

【図 7】

本発明の実施形態の磁気ディスクの製造に用いるスタンプの製造装置の説明図である。

【図 8】

本発明の実施形態の固定磁気ディスク装置の制御部の構成図である。

【図 9】

本発明の実施形態の磁気ディスクのメディア個別情報の書込み装置の構成図である。

【図 1 0】

本発明の実施形態の固定磁気ディスク装置において磁気ディスクに格納された I D 情報を読み出す手順を示すフローチャートである。

【図 1 1】

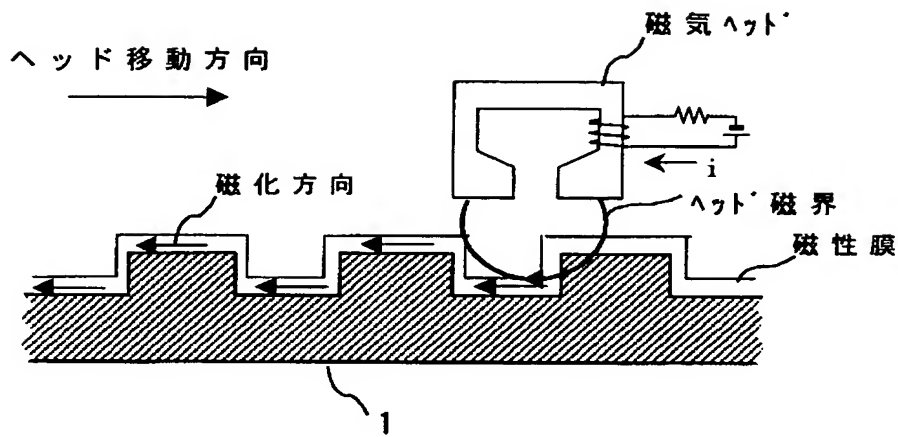
本発明の実施形態の固定磁気ディスク装置に保管する鍵テーブルの内容を示す図である。

【符号の説明】

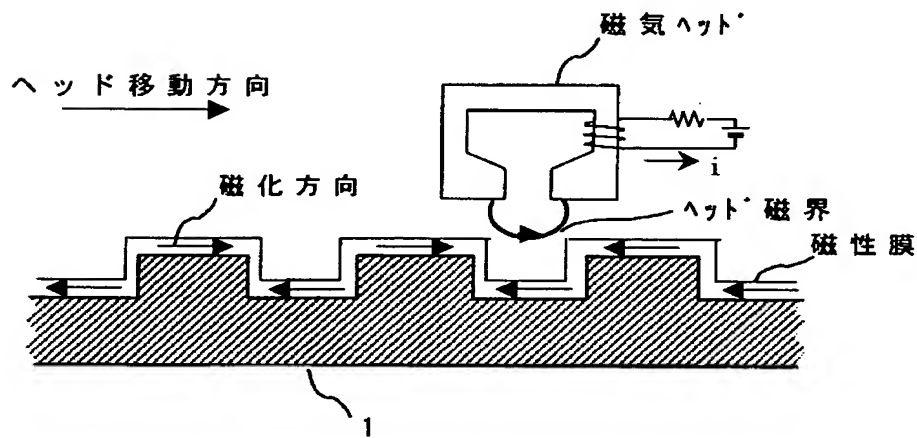
- 1 磁気ディスク
- 2 サーボゾーン
- 3 マスタ I D 情報
- 4 メディア個別 I D 情報

【書類名】 図面

【図1】

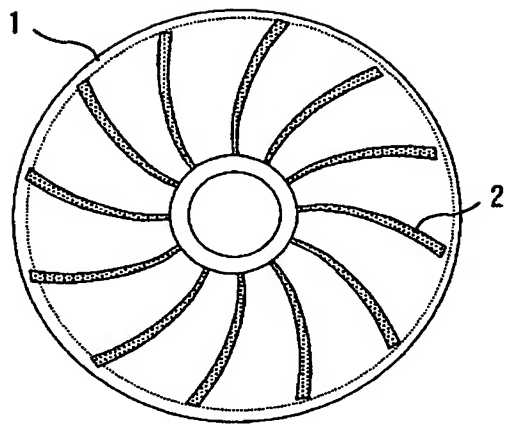


(a) 一次着磁

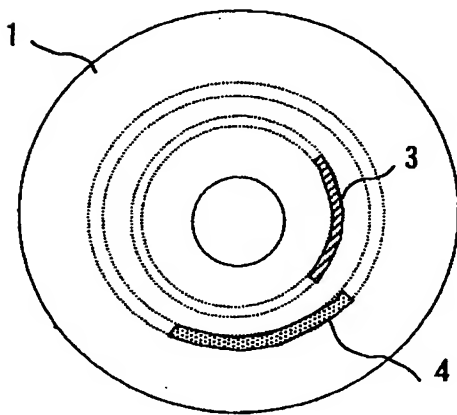


(b) 二次着磁

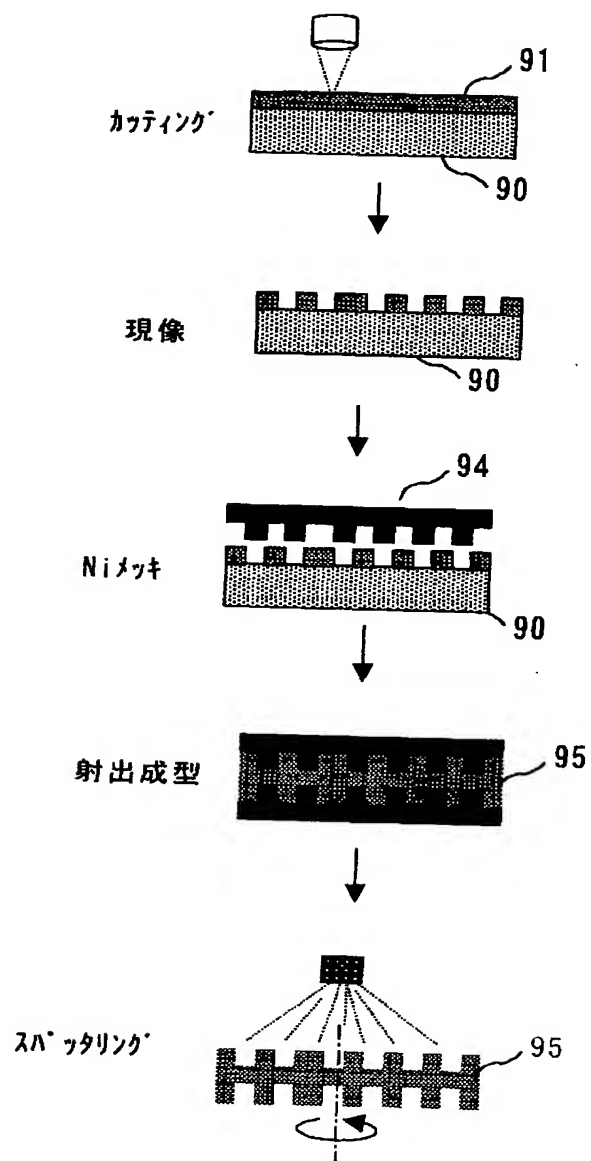
【図 2】



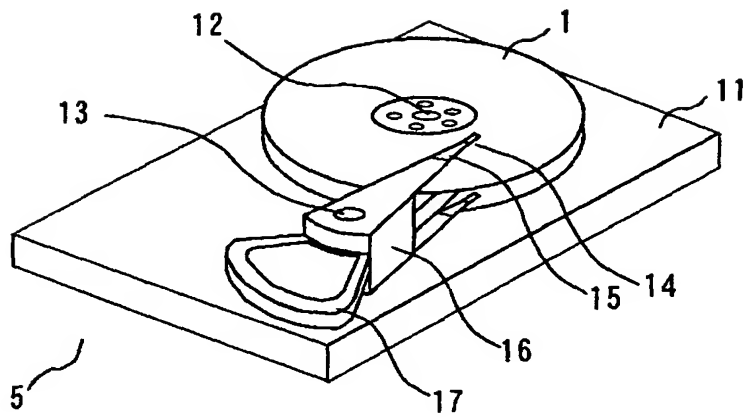
【図 3】



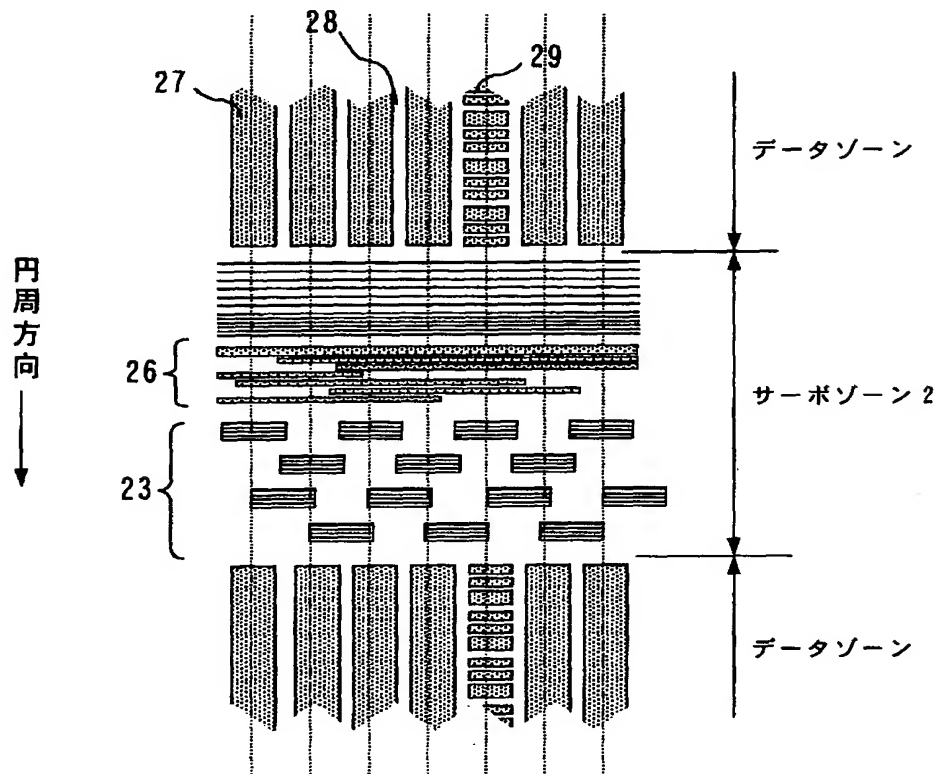
【図4】



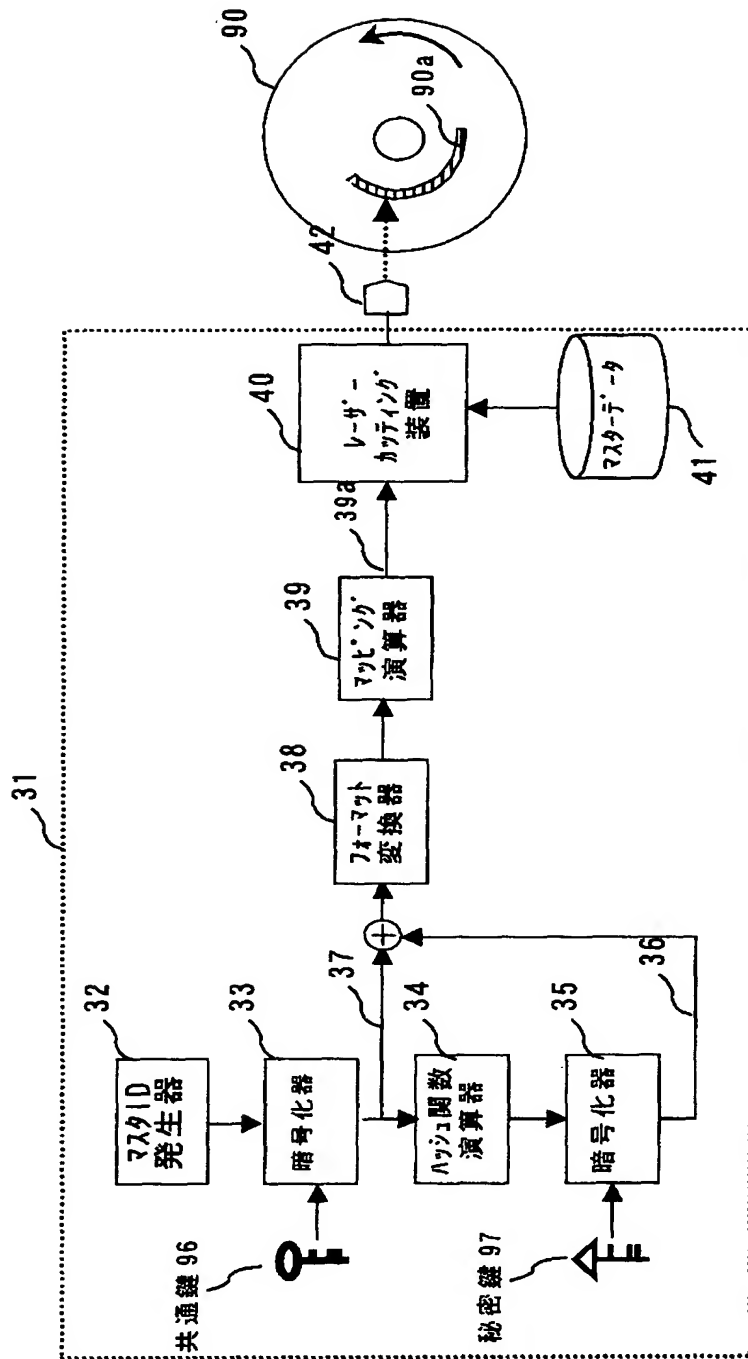
【図 5】



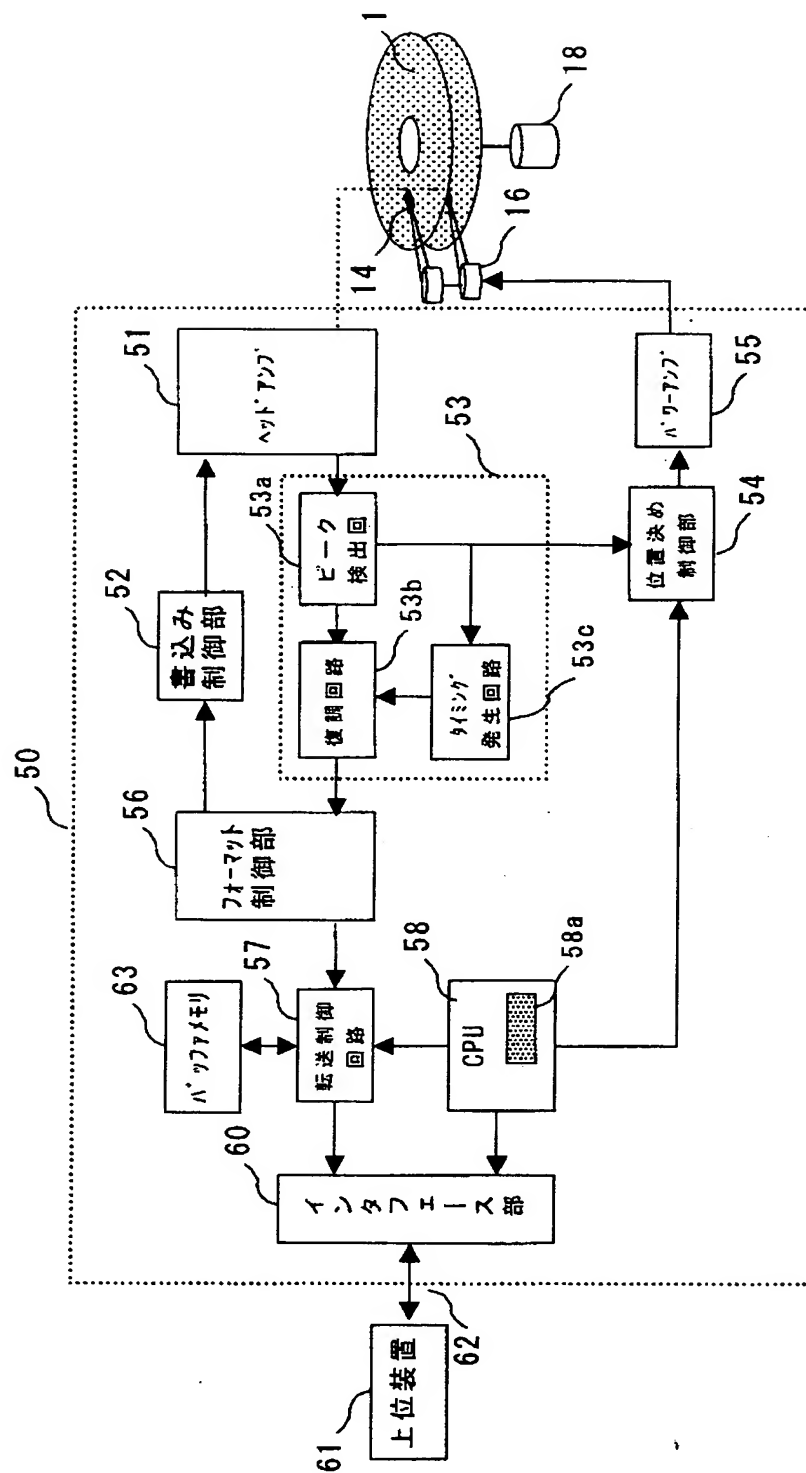
【図 6】



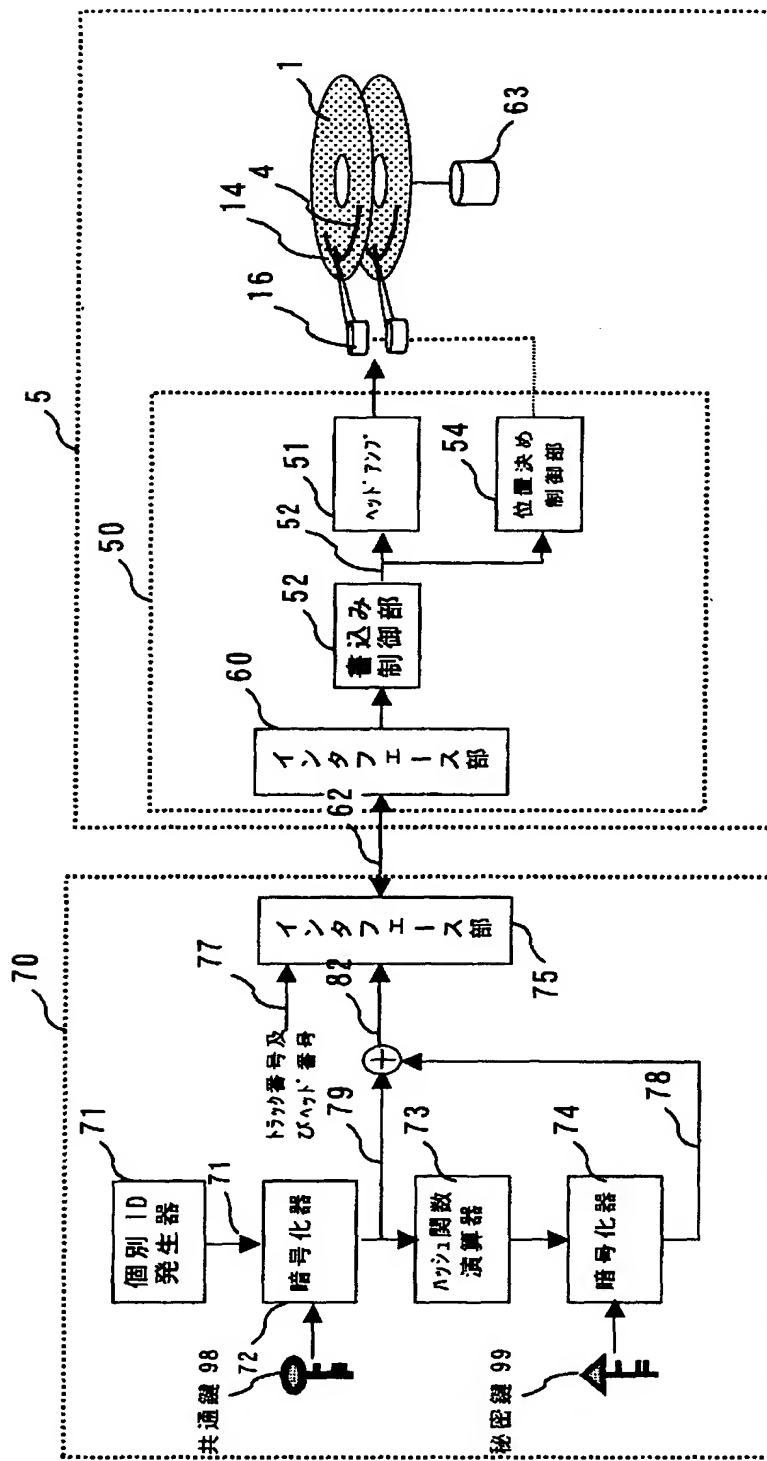
【図 7】



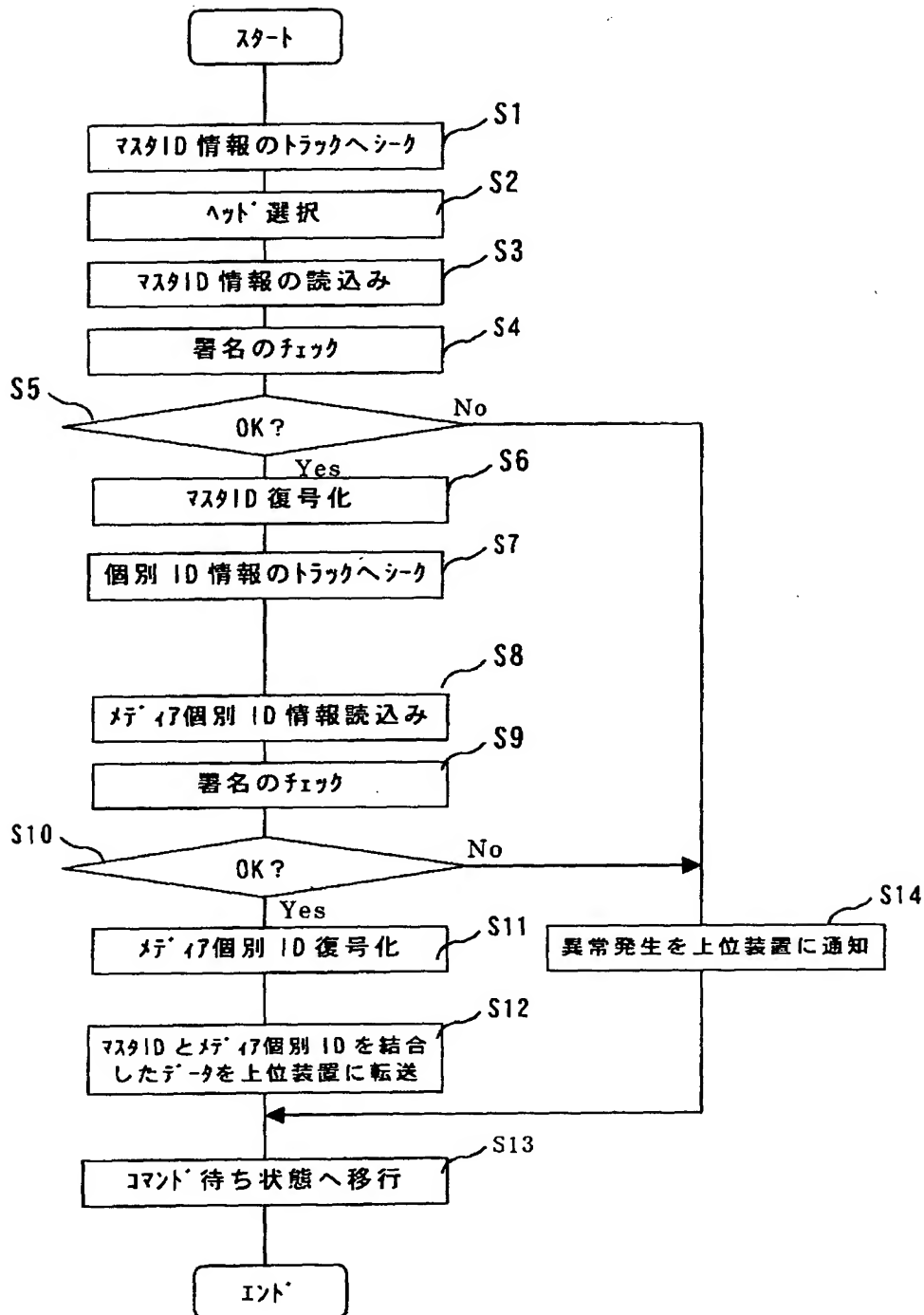
【図8】



【図9】



【図10】



【図 11】

101

| No. | 内容 | |
|-----|----------------|------|
| 1 | マスタ ID 用共通鍵 | 101a |
| 2 | マスタ ID 用公開鍵 | 101b |
| 3 | メディア個別 ID 用共通鍵 | 101c |
| 4 | メディア個別 ID 用公開鍵 | 101d |

【書類名】 要約書

【要約】

【課題】 改竄が困難であると共に、一意性の有る I D 情報を磁気ディスク媒体に埋め込むことを可能とする。

【解決手段】 メディアを一意に識別するための I D 情報を、プリエンボス型磁気ディスクのプリフォーマット領域のマスタ I D 情報 3 と、非プリフォーマット領域のメディア個別 I D 情報 4 とに分けて記録する。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000005234]

1. 変更年月日 1990年 9月 5日

[変更理由] 新規登録

住 所 神奈川県川崎市川崎区田辺新田1番1号

氏 名 富士電機株式会社